Электронный архив в банке: потребности бизнеса и соответствие правилам регулятора

Кредитные организации сдержанно относятся к возможностям хранить данные на территориально удаленных серверах, но намерены выполнять требования всех правил хранения информации.

// Андрей Лазарев, Bankir.Ru 23.07.2013 04:06
http://bankir.ru/publikacii/s/elektronnyi-arkhiv-v-banke-potrebnosti-biznesa-i-sootvetstvie-pravilam-regulyatora-10003704/

Оптимизация работы с бумажными и электронными документами и повышение эффективности основных бизнес-процессов, безусловно, одна из важнейших задач для современной банковской организации. Как следствие, в последние годы мы с вами наблюдали устойчивый рост спроса на системы работы с документами, позволяющие автоматизировать процессы документооборота и организовать электронные архивы документов.

С выходом положения ЦБ 397-П «О порядке создания, ведения и хранения баз данных на электронных носителях», предписывающего кредитным организациям обеспечить хранение информации в электронном виде, тема организации электронного архива стала еще более актуальной. Какие практические требования следуют из Положения 397-П? Как совместить требования регулятора с работой по оптимизации бизнес-процессов? У экспертов по управлению документацией, ИТ-специалистов и у банковских аналитиков-«практиков» свой взгляд и свои соображения по этому вопросу.

 Мы попросили поделиться рекомендациями ведущего эксперта по управлению документацией, члена Гильдии управляющих документацией и ARMA International **Наталью Храмцовскую**.

- Наталья Александровна, сейчас многие наши читатели, сотрудники банков, пытаются понять, что собственно от них требуется. Какие Вы могли бы дать рекомендации специалистам, на которых «свалилась» задача организовать электронный архив в соответствии с положением ЦБ 397-П и подготовить требуемые нормативные документы?

- На мой взгляд, в первую очередь важно, чтобы описываемый во внутренних нормативных документах порядок действий соответствовал тому, как эти действия на самом деле выполняются. К организации предъявляется гораздо меньше претензий в случае, когда ее сотрудники добросовестно выполняют ошибочный регламент, чем в случаях, когда при проверке выявляется несоответствие реального порядка работы соответствующим регламентам. Совершенно понятно, что сразу подготовить весь

комплект документов не получится. Предстоит большая и достаточно кропотливая работа. Основной проблемой, как мне кажется, будет нехватка методических рекомендаций на русском языке по организации хранения электронных баз данных и тем более по обеспечению сохранности информации и документов в условиях смешанного документооборота.

- И все-таки, если говорить о практических шагах, чтобы Вы посоветовали?

- На практике потребуется провести целый комплекс мероприятий, включая, например, следующие:

- Нужно заручиться поддержкой высшего руководства и разъяснить ему, зачем все это делается, в чем его персональный интерес, а также указать на возможность получения от выполняемых мероприятий отдачи для основной деятельности организации.
- Создать «команду» сотрудников из представителей нескольких специальностей (ИТ, ИБ, юристы и специалисты ДОУ и архива) для разработки плана реализации требований ЦБ и подготовки соответствующих внутренних нормативных документов банка.
- Провести инвентаризацию информационных активов организации, сохранность которых необходимо обеспечить. Выявить ту информацию, которую нужно переводить в базы данных и которая хранится в настоящее время на других носителях информации.
- Разработать или доработать внутреннюю нормативную базу, регламентирующую хранение документов и информации кредитной организации в смешанном документообороте. Центральный банк в своем положении 397-П в достаточно общем виде перечислил, какие виды нормативных документов следует разработать.
- Совершенно понятно, что сразу подготовить весь комплект документов не получится. Предстоит большая и достаточно кропотливая работа. Основной проблемой, как мне кажется, будет нехватка методических рекомендаций на русском языке по организации хранения электронных баз данных и тем более по обеспечению сохранности информации и документов в условиях смешанного документооборота.
- Принять меры организационного характера, в том числе заранее продумать порядок работы в том случае, если Банк России затребует резервные копии, и утвердить этот регламент. В частности, следует определить, кто и какие базы данных будет готовить к копированию и передаче в Банк России. Это тем более важно, поскольку Положение явным образом данный вопрос не регламентирует.
- Провести обучение персонала новым правилам работы с документами (в настоящее время ряд организаций в Москве проводят курсы повышения квалификации по тематике «Электронные документы в управлении» и «Электронные архивы»).

К номенклатуре дел все уже привыкли, однако если мы переходим к созданию электронного архива, то нужно продумать стабильную классификационную схему, рассчитанную на длительное использование, рассмотрев в том числе вопрос о возможности ее создания по функциональному, а не по структурному признаку.

Кроме того, стоит оценить, какие материалы, которые сейчас не требуется хранить в базах данных в электронном виде, имело бы смысл перевести в электронный вид, в расчете на то, что это может дать значительную отдачу в виде более эффективной и оперативной работы.

Чтобы выполнить требования Банка России в отношении резервного копирования, нужно, с моей точки зрения, по крайне мере один комплект резервных копий хранить в территориально удаленном месте. Здесь есть о чем подумать, поскольку в резервных копиях содержится вся информация банка.

- С точки зрения создания резервных копий и вообще технологической реализации, следуют ли из положения ЦБ 397-П какие-либо требования к технологической составляющей электронного архива?

- К счастью, Банк России старается не предъявлять технологических требований. Тем не менее, некоторые пункты положения вызывают определенные вопросы. Например:

«1.2. Способ отражения в электронных базах данных информации должен обеспечить ее хранение не менее чем пять лет с даты включения в электронные базы данных и обеспечить возможность доступа к такой информации по состоянию на каждый операционный день».

Реально документы и информацию придется хранить существенно дольше, чем пять лет. Соответственно могут встать вопросы:

- Подтверждения целостности документов и информации. В случае использования усиленных электронных подписей встанет проблема проверки исторических подписей, которая может оказаться особенно неприятной из-за того, что сейчас квалифицированные сертификаты могут издавать две сотни аккредитованных УЦ.
- Миграции документов в связи с устареванием форматов, съемных носителей, а также в случае вывода информационной системы из эксплуатации и замены на новую.

Предстоит еще разобраться, что требование о «возможности доступа по состоянию на каждый операционный день» означает в отношении неструктурированной информации.

Далее,

«2.1.3. Внутренними документами кредитной организации должны быть определены способы хранения информации по учету изменений, вносимых в электронные базы данных.

Способы хранения информации по учету изменений, вносимых в электронные базы данных, должны обеспечивать возможность восстановления временной последовательности событий и действий пользователей по внесению изменений в электронные базы данных, а также возможность идентификации лиц, которые вносили данные изменения».

Это, в сущности, серьезное требование к ведению, защите и обеспечению сохранности лог-файлов.

«2.2. Порядок создания, ведения и хранения электронных баз данных должен обеспечивать поддержание электронных баз данных в актуальном состоянии, возможность восстановления информации из электронных баз данных, в том числе при наступлении обстоятельств непреодолимой силы, а также исключать возникновение условий для их порчи, утраты, заражения вредоносными кодами, несанкционированного изменения содержащейся в них информации или доступа неуполномоченных лиц».

Это – комбинация требований к наличию средств резервного копирования и восстановления (или возможности использовать внешние средства такого рода), территориально удаленному хранению резервных копий и требований по информационной безопасности (например, по проведению проверки размещаемых в системе материалов на вирусы).

Стоит подумать и о возможности автоматизации создания упоминаемого в п. 4.6 паспорта резервной копии.